АНАЛИТИЧЕСКИЙ ОТЧЕТ

КИБЕРБЕЗОПАСНОСТЬ В ЭЛЕКТРОЭНЕРГЕТИКЕ

ПОДГОТОВЛЕН РАБОЧЕЙ ГРУППОЙ ЦЕНТРА КОМПЕТЕНЦИЙ «КИБЕРБЕЗОПАСНОСТЬ» («ЭНЕРДЖИНЕТ» НТИ)

МОСКВА, 2020

ОГЛАВЛЕНИЕ

АННОТАЦИЯ

Отчёт подготовлен в целях привлечения внимания к вопросам обеспечения кибербезопасности энергетической отрасли России.

В отчёте приведены результаты изучения и сравнения ряда документов, регулирующих вопросы кибербезопасности в США и России.

Отчёт предназначен для руководителей и специалистов, работающих в сфере энергетики.

ВВЕДЕНИЕ

В соответствии с Доктриной энергетической безопасности Российской Федерации, а также общепринятыми подходами, энергетическая безопасности является важной составляющей национальной безопасности страны, поскольку энергетика связана со всеми отраслями и во многом обеспечивает их функционирование.

Доктрина выделяет вызовы, угрозы и риски энергетической безопасности России, перечисляет их последствия. Угрозы энергетической безопасности разделены на внешнеполитические, внешнеэкономические, военно-политические, трансграничные и внутренние. Приводятся риски и последствия реализации. В рамках настоящего Отчета необходимо выделить следующие из них:

- нарушение нормального функционирования организаций, в том числе организаций топливно-энергетического комплекса, и отраслей экономики Российской Федерации;
- необходимость выделения дополнительных бюджетных ассигнований на ликвидацию последствий реализации угроз энергетической безопасности;
- недостаточные темпы реагирования системы профессионального образования на изменение потребности организаций топливно-энергетического комплекса в квалифицированных кадрах;
- несоответствие технологического уровня российских организаций топливно-энергетического комплекса современным мировым требованиям и чрезмерная зависимость их деятельности от импорта некоторых видов оборудования, технологий, материалов и услуг, программного обеспечения, усугубляющаяся монопольным положением их поставщиков;
- недостаточные темпы разработки и внедрения новых средств антитеррористической защиты инфраструктуры и объектов топливно-энергетического комплекса;
- недостаточный уровень защищенности инфраструктуры и объектов топливно-энергетического комплекса от актов незаконного вмешательства и опасных природных явлений.

Среди этих угроз до последнего времени не рассматривались угрозы кибербезопасности, реализация которых может спровоцировать серьезнейшие чрезвычайные ситуации в энергетике, чреватые значительным снижением возможностей обеспечения энергоресурсами потребителей.

Вместе с тем, с каждым годом предприятия топливно-энергетического комплекса всё чаще сталкиваются с компьютерными инцидентами, в том числе являющиеся следствием компьютерных атак. Стремительное развитие информационных технологий в ТЭК и тенденция перехода к интеллектуальной энергетике делают киберугрозы одними из важнейших угроз энергетической безопасности страны. В то же время, в России до сих пор нет однозначного понимания специфики и направления кибербезопасности, хотя данное определение имеется в национальных стандартах. В отличие от большинства развитых стран, в России до сих пор не принята доктрина кибербезопасности, и, как следствие, отсутствуют соответствующие стандарты, как, например, в США: «Guidelines for Smart Grid Cyber Security» (Руководство по обеспечению кибернетической безопасности Smart Grid).

АКТУАЛЬНОСТЬ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ ЭЛЕКТРОЭНЕРГЕТИКИ

В конце января 2020 года, в рамках подготовки к ежегодной сессии Всемирного экономического форума (ВЭФ), эксперты ВЭФ опубликовали свой доклад о наиболее значимых глобальных рисках. В числе основных рисков специалисты выделили кибератаки на инфраструктуру — 76,1%.

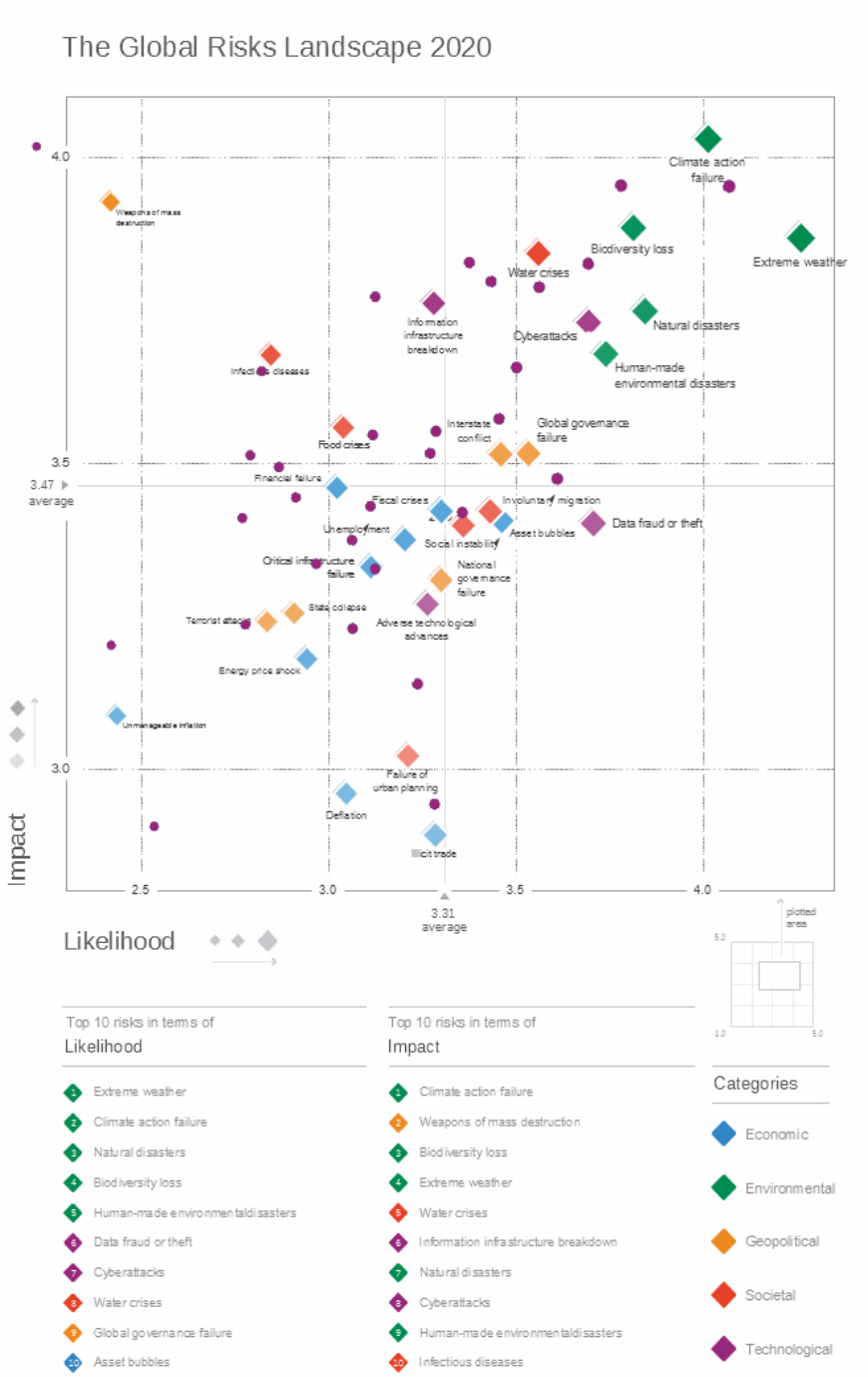

Рисунок 1. Глобальные риски

На международном уровне оценка уровня обеспечения информационной безопасности осуществляется Международным союзом электросвязи (ITU), который составляет рейтинг стран по индексу кибербезопасности с 2007 г. В рейтинг входят 194 страны-участницы ООН. По состоянию на 2018 г. 58% стран-участниц имеют национальную стратегию в области кибербезопасности, в то время как в предыдущей редакции рейтинга таких насчитывалось всего 50%. Кроме того, 91% государств имеют законодательство в этой сфере, хотя в 2017 г. таких стран было всего 79%.

В 2018 г. в рейтинге Глобального индекса кибербезопасности Global Cybersecurity Index 2018 (таб. 1) Россия заняла 26 место с показателем 0,836 балла. При этом, в предыдущей редакции рейтинга, выпущенной в 2017 г., она занимала десятое место с индексом 0,788 балла. Таким образом, Россия опустилась в списке на 16 позиций, однако сумела улучшить свои показатели.

В новом рейтинге России было начислено 0,197 балла за законодательство и наличие регулирования в области кибербезопасности, еще 0,162 балла — за технологическую сторону вопроса, 0,177 балла — за организацию на национальном уровне, 0,166 балла — за наращивание мощностей, подготовку кадров и информирование, и 0,135 балла — за международное сотрудничество. По сравнению с 2017 г. составители рейтинга отмечают в стране улучшение мер, принятых против мошенничества в сфере использования электронных платежных систем.

На первом месте рейтинга находится Соединенное королевство с показателем 0,931 балла, которая в рейтинге за 2017 г. занимала только 12 место. За ней следуют США, набравшие 0,926 балла, и Франция с результатом 0,918 балла. При этом США удалось сохранить за собой второе место, а Франция поднялась на третье с восьмого. Первую пятерку замыкают Литва и Эстония, набравшие 0,908 и 0,905 балла соответственно.

Таблица 1. Global Cybersecurity Index 2018

Рейтинг	Государство	Баллы
1	Соединенное королевство	0,931
2	Соединенные Штаты Америки	0,926
3	Франция	0,918
4	Литва	0,908
5	Эстония	0,905
6	Сингапур	0,898
7	Испания	0,896
8	Малазия	0,893
9	Канада	0,892
9	Норвегия	0,892
10	Австралия	0,890
11	Люксембург	0,886
12	Нидерланды	0,885
13	Саудовская Аравия	0,881
14	Япония	0,880
14	Маврикий	0,880
15	Республика Корея	0,873
16	Оман	0,868
17	Катар	0,860
18	Грузия	0,857
19	Финляндия	0,856
20	Турция	0,853
21	Дания	0,852
22	Германия	0,849
23	Египет	0,842
24	Хорватия	0,840
25	Италия	0,837
26	Российская Федерация	0,836

ПОЗИЦИЯ РЕГУЛЯТОРОВ И ОТРАСЛИ В ОТНОШЕНИИ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ

Согласно данным Исследования Российского энергетического агентства, вопросы информационной безопасности в энергетике требуют значительно проработки (Рис. 2).

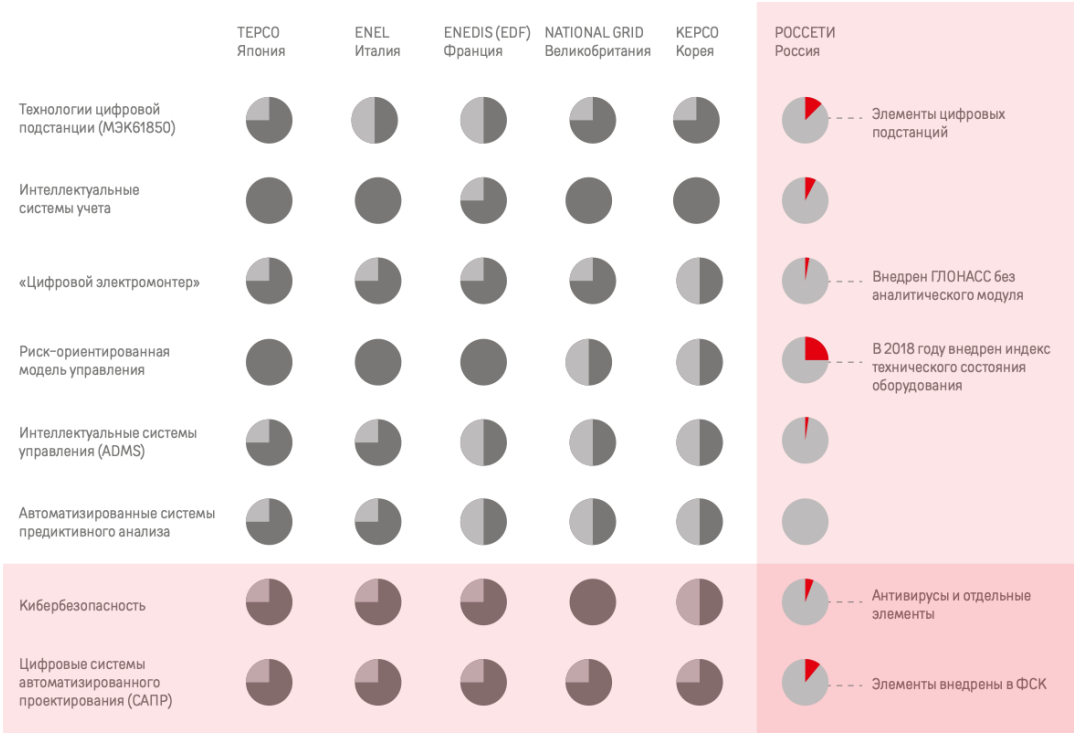

Рисунок 2. Исследования Российского энергетического агентства, аналитические материалы Ernst and Young (2017, 2018)

В сентябре 2019 г. в рамках Kaspersky Industrial Cybersecurity Conference 2019, Евгений Грабчак - Директор Департамента оперативного контроля и управления в электроэнергетике Минэнерго России (в настоящее время — замминистра энергетики) - дал рекомендации субъектам ТЭК в части защиты объектов критической информационной инфраструктуры, ключевыми из которых являются необходимость категорирования объектов КИИ, создание модели угроз и разработка типовых мер реагирования при кибератаке. Директор Департамента отметил важность систематического анализа готовности и устойчивости, по результатам которого должна производиться оценка уязвимости компонентов инфраструктуры обмена данными и актуализация внутренних регламентов кибербезопасности. При этом особое внимание необходимо уделять проведению учебных мероприятий в целях отработки действий по обеспечению информационной безопасности при различных сценариях развития, а также совершенствованию механизмов раннего предупреждения экстренного реагирования.

НОРМАТИВНОЕ ОБЕСПЕЧЕНИЕ

Необходимо отметить, что в США, Соединенном королевстве и ряде других стран различаются понятия «Критическая инфраструктура (Critical infrastructure)» и «Критическая информационная инфраструктура (Critical information infrastructure», имеется большое количество нормативно-правовых актов, а также рекомендации (лучшие практики) по идентификации критических активов и обеспечению безопасности, выпускаемые как государственными, так и общественными организациями (см. «Источники информации» [8-14]).

Критическая инфраструктура, также называемая национально значимой инфраструктурой, может быть в широком смысле определяется как системы, активы, средства и сети, которые предоставляют основные услуги и необходимы для национальной безопасности, экономической безопасности, процветания, здоровья и безопасности соответствующих стран. Влияние: терроризм и стихийные бедствия, изменение климата и демографические сдвиги

В качестве примера для электроэнергетики можно привести раздел на сайте ENISA:

- Smart Grid as part of Critical Infrastructures and Services
- Smart Grid Security Certification in Europe
- Smart Grid Security: Recommendations for Europe and Member States
- Appropriate security measures for smart grids
- Communication network interdependencies in smart grids

РЕГУЛИРОВАНИЕ ВОПРОСОВ КИБЕРБЕЗОПАСНОСТИ В ЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ США

Необходимо отметить, что вопросы обеспечения информационной безопасности критической инфраструктуры (критически важных объектов и т. п., в состав которой входит критическая информационная инфраструктура КИИ / CII) в последнее время находятся в сфере пристального внимания руководства практически всех промышленно развитых стран.

На основании собранных и проанализированных группой материалов, представляется, что законодательство в указанной области наиболее развито в Соединенных Штатах Америки, при этом законодательные органы других стран стараются гармонизировать свои нормативные документы с американскими. С точки зрения нормативного обеспечения вопросов регулирования кибербезопасности в США последние несколько лет характеризовались интенсивной и целенаправленной деятельностью. В событийном плане данный период можно считать начавшимся с февраля 2013 г., когда был принят Executive Order 13636 «Improving Critical Infrastructure Cybersecurity», и завершившимся в сентябре 2018 г., когда была принята Стратегия кибербезопасности США.

При этом в США регулирование вопросов кибербезопасности осуществляется не только на федеральном уровне, но и на уровне отдельных отраслей промышленности, в частности в энергетической сфере. При этом возникла система документов, детализирующих общегосударственную политику обеспечения кибербезопасности, а разработчиком и, в определенной степени регулятором, выступило Министерство энергетики США (Department of Energy, DOE).

В результате указанной деятельности был разработан целый комплекс документов, затрагивающий, в том числе, вопросы регулирования в энергетическом секторе. Всего по линии Министерства энергетики США за указанный период были приняты следующие документы:

1. Cybersecurity capability maturity model (C2M2). Февраль 2014 г.
2. 2015 Energy Sector-Specific Plan (SSP). 2015 г.
3. DOE Multiyear Plan for Energy Sector Cybersecurity. Март 2018 г.
4. Cybersecurity strategy 2018-2020. Июнь 2018 г.
5. Securing Energy Infrastructure Act. Сентябрь 2019

Стоит отметить, что разработка комплекса документов велась «снизу-вверх», когда документ стратегического планирования появился в качестве завершающего в формируемой иерархии нормативной базы.

Рассмотрим более подробно Стратегию кибербезопасности 2018-2020 Министерства энергетики США. Содержание документа может быть описано схемой, представленной на рис. 3.

Рисунок 3. Основные цели стратегии кибербезопасности

В документе раскрываются обозначенные на схеме понятия.

Цель 1.1. Безопасный и надежный доступ к информации

Для достижения успеха миссии [обеспечения кибербезопасности] сотрудники Министерства энергетики США (далее МЭ США) и заинтересованные стороны должны иметь безопасный и надежный доступ к необходимым для выполнения миссии системам, сетям и информационным ресурсам.

Цель 2.1. Определение - расширение организационных возможностей для управления рисками кибербезопасности.

Executive Order (EO) 13800 предписывает руководству [Министерства] внедрить меры по управлению рисками и обеспечить, чтобы процессы управления рисками кибербезопасности были согласованы с процессами стратегического, оперативного и бюджетного планирования. Для того, чтобы регулировать деятельность, связанную с риском кибербезопасности в масштабах всего предприятия, Министерство энергетики США использует установленные руководящие принципы, в том числе такие документы как Cybersecurity Capability Maturity Model (Модель зрелости потенциала кибербезопасности), Cybersecurity Evaluation Tool (Инструмент оценки кибербезопасности), и Electricity Subsector Cybersecurity Risk Management Process (Процесс управления рисками кибербезопасности подсектора электроэнергетики).

Цель 2.2. Защита - разработка и внедрение общеорганизационных мер контроля для снижения рисков и повышения осведомленности о кибербезопасности предприятий посредством развития и обучения рабочей силы.

МЭ США продолжает разрабатывать требования и соответствующие решения для обеспечения безопасности информационных ресурсов. Они охватывают стандарты и передовую практику, независимо от происхождения, если они могут привести к повышению эффективности работы, снижению затрат и более быстрой интеграции инновационных ИТ-решений.

Цель 2.3. Обнаружение - разработка инструментов и процессов для ускорения уведомления об угрозах кибербезопасности.

МЭ США использует лучшие в своем классе инструменты, необходимые для сокращения времени обнаружения киберугроз, уведомления и реагирования на уровне отрасли. Организационно это реализовано в виде интегрированного совместного Координационного центра кибербезопасности (iJC3), обеспечивающего единый и стандартизированный подход к сбору данных о кибербезопасности и совместной аналитике в режиме реального времени. При этом данный подход не препятствует отдельным предприятиям разрабатывать уникальные стратегии кибербезопасности в соответствии с их целями.

Цель 2.4. Реагирование - быстрый анализ аномалий и предполагаемых событий и реагирование на них.

Для эффективной борьбы с постоянно развивающимися угрозами МЭ США необходимо разработать свою Программу управления инцидентами в области кибербезопасности, включающую расширение аналитической криминалистики и тактики реагирования, использование автоматизированных инструментов для оптимизации обеспечения безопасности информационных технологий, улучшение возможностей управления инцидентами и проведение обучения полевых операторов. С этой целью в сотрудничестве с федеральным правительством и энергетическим сектором МЭ США разрабатывает передовые решения кибербезопасности для укрепления и координации возможности реагирования на инциденты и совместное использование ресурсов.

Цель 2.5. Восстановление - разработка и внедрение процесса разбора инцидентов, реагирования и восстановления для нейтрализации и устранения угроз кибербезопасности.

МЭ США будет стремиться поддерживать элементы кибербезопасности и согласовывать свои усилия по обеспечению устойчивости в соответствии с PPD 40, Федеральной директивой о непрерывности (FCD) 1 & 2 и Национальной программой непрерывности Федерального агентства по чрезвычайным ситуациям (FEMA).

Цель 3.1 - Клиентоориентированная кибербезопасность.

Эффективные меры кибербезопасности должны согласовываться и должны быть адаптированы, где это возможно, к специализированным требованиям клиентов, потребностям и способам ведения бизнеса.

Цель 4.1 – Риск ориентированный подход.

В соответствии с FISMA и EO 13800, а также Cybersecurity Framework, Стратегия кибербезопасности придерживается риск ориентированного подхода. Прагматизм требует, чтобы МЭ США уделяло приоритетное внимание своим ограниченным ресурсам для удовлетворения важнейших потребностей миссии, сознавая при этом последствия событий кибербезопасности.

Анализ приведенного документа (Стратегии МЭ США), а также основного документа для принятия технических решений – Cybersecurity Framework показывает, что основные стратегические решения по управлению рисками реализуются на уровне предприятий. При этом, как было заложено в EO 13636, вопросы повышения уровня кибербезопасности носят добровольный характер.

РЕГУЛИРОВАНИЕ ВОПРОСОВ КИБЕРБЕЗОПАСНОСТИ В ЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Несмотря на актуальность темы кибербезопасности для промышленных предприятий на сегодняшний день в Российской Федерации не существует взаимоувязанных методических и организационно распорядительных документов, позволяющих выполнять комплексное построение и эксплуатацию объектов и систем электроэнергетики как комплексных киберфизических систем. Как пример, невозможно техногенный инцидент идентифицировать как следствия кибератаки или иного компьютерного инцидента, что в дальнейшем приводит к отсутствию проблемы кибербезопасности как таковой в нормативном поле.

Вопросы компьютерных атак на киберфизические системы рассматриваются исключительно в разрезе информационной безопасности. В настоящее время основным документом стратегического планирования в области обеспечения информационной безопасности Российской Федерации является Доктрина информационной безопасности, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 г. № 646 (далее – Доктрина). В данном документе текущее состояние информационной безопасности и направления обеспечения информационной безопасности рассматриваются в разрезе стратегических национальных приоритетов, обозначенных в новой Стратегии национальной безопасности Российской Федерации, что должно в перспективе позволить выстраивать всю иерархию документов в сфере информационной безопасности с учетом соответствующих стратегических национальных приоритетов.

Следует отметить, что в Доктрине экономическая сфера обеспечения информационной безопасности сосредоточена именно на важности и необходимости формирования отрасли информационных технологий и информационной безопасности. Говоря другими словами, сфера информационных технологий рассматривается как непосредственная часть жизни общества.

Еще одним не менее важным нововведением Доктрины информационной безопасности являются усовершенствованные задачи государственных органов в рамках деятельности по формированию и усовершенствованию системы обеспечения информационной безопасности, а именно:

- укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;
- совершенствование форм и методов взаимодействия сил обеспечения информационной безопасности в целях повышения их готовности к противодействию информационным угрозам, в том числе путем регулярного проведения тренировок (учений);
- совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;
- повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности.

В связи с растущим уровнем угроз информационной безопасности, в новой Доктрине уделяется внимание такому вопросу, как защита критической информационной инфраструктуры Российской Федерации, делается упор на обеспечение ее бесперебойного и устойчивого функционирования.

В части законодательства Российской Федерации, основным документом, регулирующим вопросы обеспечения защиты от компьютерных атак на автоматизированные системы промышленных объектов и объектов ТЭК является Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». При этом, обеспечение информационной безопасности электроэнергетики регламентируется следующими основными подзаконными актами и документами:

- Приказ ФСТЭК России №235 от 21.12.2017 (ред. 27.03.2019) «Об утверждении Требований к созданию систем безопасности значимых объектов КИИ РФ и обеспечению их функционирования»;
- Приказ ФСТЭК России №239 от 25.12.2017 (ред. 26.03.2019) «Об утверждении Требований по обеспечению безопасности значимых объектов КИИ РФ»;
- Приказ ФСБ России №367 от 24.07.2018 «Об утверждении Перечня информации, представляемой в ГосСОПКА и Порядка представления информации в ГосСОПКА»;
- Приказ ФСБ России №196 от 06.05.2019 «Об утверждении требований к средствам ГосСОПКА»;
- Приказ Министерства энергетики РФ от 6 ноября 2018 г. № 1015 «Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования» (СУМиД).

Помимо вышеуказанных нормативных правовых актов к документам по обеспечению безопасности объектов критической информационной инфраструктуры можно отнести приказ
ФСТЭК России №31 от 14.03.2014 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды», требования которого распространяются на безопасность АСУ критически важных и потенциально опасных объектов, которым не присвоена категория как объектам КИИ.

Кроме того, в соответствии с требованиями статьи 11 ФЗ-256 от 21.07.2011 г. «О безопасности объектов ТЭК» и в целях обеспечения безопасности объектов топливно-энергетического комплекса субъекты ТЭК создают на этих объектах системы защиты информации и информационно-телекоммуникационных сетей от неправомерных доступа, уничтожения, модифицирования, блокирования информации и иных неправомерных действий и обеспечивают функционирование таких систем.

Министерством энергетики РФ при активном участии компаний топливно-энергетического комплекса сформирован ведомственный проект «Цифровая энергетика», направленный на создание условий для внедрения в отрасли цифровых технологий и платформенных решений, с учетом приоритетов, обозначенных Президентом Российской Федерации, и положений утвержденной в 2017 году национальной программы «Цифровая экономика Российской Федерации». В задачи единой технической политики проекта «Цифровая энергетика» входит определение единой политики по обеспечению информационной и кибербезопасности в единой отраслевой информационной среде.

Также вопросы кибербезопасности киберфизических систем электроэнергетике были рассмотрены в 2016-2019 годах исследовательскими комитетами B5 и D2 РНК СИГРЭ, для этого была создана проблемная рабочая группа «Кибербезопасность РЗА и систем управления современных объектов электроэнергетики». К результатам работы можно отнести впервые разработанную методологию формирования базовой модели угроз кибербезопасности в разрезе функциональной безопасности объектов электроэнергетики. В основу базовой модели угроз кибербезопасности киберфизических систем управления в электроэнергетике положен перечень аварий, перечисленных в Постановлении Правительства от 28 октября 2009 г. N 846 «Об утверждении Правил расследования причин аварий в электроэнергетике» от 28.10.2009 (с учетом изменений, принятых Постановлением Правительства РФ № 525 от 10.06.2016). Особенностью предложенной модели угроз является смещение акцентов от классических угроз информационной безопасности в сторону киберфизической модели объекта. Особое внимание уделялось влиянию на оперативное управление, противоаварийные защитные функции и физический вывод из работы первичного и вторичного оборудования электроэнергетики.

СРАВНЕНИЕ ВОПРОСОВ РЕГУЛИРОВАНИЯ КИБЕРБЕЗОПАСНОСТИ

Если сравнивать систему обеспечения кибербезопасности критической (информационной) инфраструктуры в США с системой, выстроенной в Российской Федерации в соответствии с 187-ФЗ, можно выделить элементы сходства, но и различия.

В США, как уже было отмечено, основные решения по управлению рисками возложены на собственников и операторов критической инфраструктуры. При этом государственные органы обеспечивают указанных лиц информацией об угрозах, а также о стандартах управления рисками, возможных решениях и лучших практиках.

В Российской Федерации при организации государственной системы обеспечения кибербезопасности также присутствует этап по управлению рисками, но он носит своеобразный характер и заключается в процедуре категорирования объектов критической информационной инфраструктуры. После определения категории значимости (если такая категория значимости была присвоена), собственники и операторы объекта критической информационной инфраструктуры должны в обязательном порядке реализовать требования по информационной безопасности, разработанные регуляторами, которые не предусматривают вариативности или какого-либо управления рисками.

Данная процедура хотя технически реализуется сотрудниками предприятий, но в условиях государственного контроля фактически обеспечивает интересы государства. Говоря другими словами, процесс стратегического управления рисками каждого конкретного предприятия осуществляется государством.

ВЫВОДЫ

Развитие электроэнергетики невозможно без внедрения цифровых технологий (построения современных систем управления), а, следовательно, и глубокой проработки вопросов обеспечения кибербезопасности. Решения, разрабатываемые сегодня и в ближайшие 10 лет, должны быть фундаментально пересмотрены в концептуальном, методологическом, технологическом и организационном разрезе. В экосистему (сферу) электроэнергетики должны быть включены вопросы кибербезопасности.

Также требуется выстроить диалог и содействие между участниками сферы электроэнергетики в части вопросов регулирования вопросов кибербезопасности.

Для решения данных вопросов кибербезопасности на базе НТИ «Энерджинет» сформирован центр компетенций «Кибербезопасность», объединяющий широкий круг специалистов:

- Представителей отрасли: Минэнерго России, АО «СО ЕЭС»
- Теоретиков и практиков из научных и образовательных учреждений: РГУ нефти и газа (НИУ) имени И.М. Губкина, ФРАОУ ДПО «ИПК ТЭК»
- Производителей решений информационной безопасности: Kaspersky, InfoWatch Интеграторов в сфере ИБ и ИТ: Ростелеком Солар, Igrids, Ангара технолоджис.

Будем рады сотрудничеству!

https://energynet.ru/?p=dcenter

Отчет подготовлен рабочей группой в составе: А.Ю. Гуревич, А.В. Петухов, Д.И. Правиков, М.Б. Смирнов, А.Ю. Юршев

ПРИЛОЖЕНИЕ 1

СПРАВОЧНЫЕ МАТЕРИАЛЫ ПО ОСНОВНЫМ ФЕДЕРАЛЬНЫМ ЗАКОНАМ РОССИЙСКОЙ ФЕДЕРАЦИИ.

ТРЕБОВАНИЯ ФЗ-256 ОТ 21.07.2011 Г. «О БЕЗОПАСНОСТИ ОБЪЕКТОВ ТЭК»

В статье 11 ФЗ-256 от 21.07.2011 г. «О безопасности объектов ТЭК» указано, что «В целях обеспечения безопасности объектов топливно-энергетического комплекса субъекты топливно-энергетического комплекса создают на этих объектах системы защиты информации и информационно-телекоммуникационных сетей от неправомерных доступа, уничтожения, модифицирования, блокирования информации и иных неправомерных действий и обеспечивают функционирование таких систем. Создание таких систем предусматривает планирование и реализацию комплекса технических и организационных мер, обеспечивающих в том числе антитеррористическую защищенность объектов топливно-энергетического комплекса».

Под **объектом топливно-энергетического комплекса** здесь понимаются объекты электроэнергетики, нефтедобывающей, нефтеперерабатывающей, нефтехимической, газовой, угольной, сланцевой и торфяной промышленности, а также объекты нефтепродуктообеспечения, теплоснабжения и газоснабжения.

Для уточнения понятия «Объект ТЭК» приведены некоторые определения.

В соответствии с ФЗ№35 от 26.03.2002 «Об электроэнергетике»:
объекты электроэнергетики - имущественные объекты, непосредственно используемые в процессе производства, передачи электрической энергии, оперативно-диспетчерского управления в электроэнергетике и сбыта электрической энергии, в том числе объекты электросетевого хозяйства;
объекты электросетевого хозяйства - линии электропередачи, трансформаторные и иные подстанции, распределительные пункты и иное предназначенное для обеспечения электрических связей и осуществления передачи электрической энергии оборудование;

В соответствии с ФЗ-190 от 27.07.2010 «О теплоснабжении»:
объекты теплоснабжения - источники тепловой энергии, тепловые сети или их совокупность;
источник тепловой энергии - устройство, предназначенное для производства тепловой энергии;
тепловая сеть - совокупность устройств (включая центральные тепловые пункты, насосные станции), предназначенных для передачи тепловой энергии, теплоносителя от источников тепловой энергии до теплопотребляющих установок.

Исходя из приведенных определений ясно, что «объектом ТЭК» является оснащенное соответствующим оборудованием производственное подразделение предприятия, например подстанция или тепловой пункт. Такие объекты, как ТЭЦ, судя по определению, содержат в своём составе как объекты электроэнергетики, так и объекты теплоснабжения, также являются объектами ТЭК.

Объекты электроэнергетики (линии передачи электрической энергии, оперативно-диспетчерского управления в электроэнергетике, объекты электросетевого хозяйства - линии электропередачи, трансформаторные и иные подстанции, распределительные пункты и иное предназначенное для обеспечения электрических связей и осуществления передачи электрической энергии оборудование) также являются производственными подразделениями профильных предприятий.

Таким образом, требования статьи 11 ФЗ-256 от 21.07.2011 г. «О безопасности объектов ТЭК» относятся к производственным подразделениям профильных предприятий. Указанные подразделения могут располагаться локально: в отдельных помещениях, зданиях или территориях, где обычно там же расположено производственное/диспетчерское оборудование или его часть, часть оборудования может быть расположена отдельно или представлять собой линейный объект.

Отсюда, для выполнения вышеприведенных требований необходимо создать системы защиты информации и информационно-телекоммуникационных сетей (ИТС) не только в части систем управления производственным (технологическим) оборудованием, а для производственных подразделений профильных предприятий ТЭК в целом.

Указанные объекты защиты (информация и ИТС) в таких подразделениях могут быть в составе не только АСУТП, но и инженерно-технических средств охраны (ИТСО), а также размещенных на таких объектах сегментах корпоративных систем, которые, в свою очередь, в зависимости от локализации иных подразделений и степени сегментации эксплуатируемых ими систем, могут включать MES, PLM, ERP и т.п.

Требования по информационной (кибер) безопасности вышеприведенных систем могут содержаться в различных документах в зависимости от как самих систем, так и от обрабатываемой ими информации. Для АСУТП критически важных объектов (КВО), к которым относятся объекты ТЭК необходимо использовать Приказ ФСТЭК от 14 марта 2014 г. №31 (ред. от 5.09.2018) «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды». Для объектов ТЭК, не являющихся КВО, требований по информационной безопасности, приведенных в приказах ФСТЭК или иных ФОИВ нет, как нет их и для таких систем, как ИТСО. Для этих и иных корпоративных систем требования по информационной безопасности определяются корпоративными документами (политиками информационной безопасности, технической политикой, стандартами предприятия), в том числе по защите коммерческой тайны, персональных данных и иной конфиденциальной информации. Требования по защите персональных данных, также определяются профильным ФЗ-152 от 27.07.2006 г. «О защите персональных данных» и его подзаконных актах. Указанные требования необходимо выполнять в том случае, если персональные данные содержатся/обрабатываются в указанных системах и на предприятии в целом. На предприятии также может обрабатываться информация, содержащая коммерческую тайну, поэтому с учетом требования ст. 11 ФЗ-187, необходимо ввести соответствующий режим (ФЗ-98 от 29.07.2004 «О коммерческой тайне»), выпустить и обеспечить выполнение ряда организационно-распорядительных документов (перечень информации …, инструкция о конфиденциальном делопроизводстве, инструкции и пр.).

ТРЕБОВАНИЯ ФЗ-187 ОТ 26.07.2017 «О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РФ» И ЕГО ПОДЗАКОННЫХ АКТОВ

С изданием этого закона внесены изменения в следующие документы:

- Закон Российской Федерации от 21 июля 1993 года № 5485-I «О государственной тайне» (пункт 4 статьи 5).
- Федеральный закон от 7 июля 2003 года № 126-ФЗ «О связи» (пункт 11 статьи 12, пункт 1 статьи 46).
- Федеральный закон от 26 декабря 2008 года № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» (часть 31 статьи 1).
- Уголовный кодекс Российской Федерации (статья 274-1).
- Уголовно-процессуальный кодекс Российской Федерации (статья 151).

В соответствии с указом Президента Российской Федерации от 25.11.2017 № 569 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента Российской Федерации от 16 августа 2004 г. №1085», федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры (КИИ) Российской Федерации, является Федеральная служба по техническому и экспортному контролю.

В соответствии с указом Президента Российской Федерации от 22.12.2017 г. №620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», на Федеральную службу безопасности Российской Федерации возложены функции федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Помимо вышеприведенного закона, ряд требований к защите объектов КИИ содержится в ряде приказов ФСТЭК РФ и ФСБ России, постановлений Правительства РФ, в том числе:

- Приказ ФСТЭК России от 21 декабря 2017 г. №235 (ред. от 13.06.2019) «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».
- Приказ ФСТЭК России от 25 декабря 2017 г. №239 (ред. от 18.04.2019) «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

- Приказ ФСТЭК России от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации».

- Приказ ФСТЭК России от 22 декабря 2017 г. N 236 (ред. от 21.03.2019) «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

- Приказ ФСТЭК России от 11 декабря 2017 г. N 229 «Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

- Приказ Федеральной службы безопасности Российской Федерации от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам».

- Приказ Федеральной службы безопасности Российской Федерации от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения».

- Приказ Федеральной службы безопасности Российской Федерации от 06.05.2019 № 196 «Об утверждении требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты».

- Приказ Федеральной службы безопасности Российской Федерации от 19.06.2019 № 281 «Об утверждении Порядка, технических условий установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры Российской Федерации».

- Приказ Федеральной службы безопасности Российской Федерации от 24.07.2018 № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

- Приказ Федеральной службы безопасности Российской Федерации от 16.07.2019 № 282 «Об утверждении Порядка информирования ФСБ России о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации».
- Постановление Правительства Российской Федерации от 08.02.2018 № 127 (ред. от 13.04.2019) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».
- Постановление Правительства Российской Федерации от 17.02.2018 № 162 «Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
- Постановление Правительства Российской Федерации от 08.06.2019 № 743 «Об утверждении Правил подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры».

В соответствии с законом, к объектам КИИ относятся информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сферах:

- здравоохранения,
- науки,
- транспорта,
- связи,
- энергетики,
- банковской сфере и иных сферах финансового рынка,
- топливно-энергетического комплекса,
- в области атомной энергии,
- оборонной,
- ракетно-космической,
- горнодобывающей,
- металлургической и химической промышленности.

Объекты КИИ учитываются в отдельном государственном реестре (приказ ФСТЭК России от 22 декабря 2017 г. №236, приказ ФСТЭК России от 06.12.2017 г. №227) и подлежат категорированию, всего существует 3 категории. Критерии категорирования и его порядок приведены в постановлении Правительства Российской Федерации от 08.02.2018 №127. Для значимых объектов КИИ необходимо создавать системы и подсистемы безопасности.

Основными задачами системы безопасности значимого объекта критической информационной инфраструктуры являются:

1. предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

2. недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта критической информационной инфраструктуры;

3. восстановление функционирования значимого объекта критической информационной инфраструктуры, обеспечиваемого в том числе за счет создания и хранения резервных копий необходимой для этого информации;

4. непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Для коммерческих организаций, к которым относятся большинство объектов КИИ объектов ТЭК, пока не установлены сроки начала категорирования (отправки во ФСТЭК РФ перечня объектов КИИ, подлежащих категорированию). Само категорирование должно быть проведено не позже одного года после отправки такого перечня, а плановые проверки, проводимые соответствующими ФОИВ – не ранее трех лет с даты внесения значимых объектов в соответствующий реестр.

Системы безопасности (силы, средства и организационно-распорядительные документы) создаются в соответствии с приказом ФСТЭК России от 21 декабря 2017 г. №235, а подсистемы безопасности (совокупность организационных и технических мер) - в соответствии с приказом ФСТЭК России от 25 декабря 2017 г. №239.

Системы безопасности создаются незамедлительно для всех значимых объектов КИИ после их категорирования, а подсистемы – также, или по отдельному плану модернизации значимых объектов КИИ и/или их систем безопасности, если такие подсистемы уже были созданы на объектах, отнесенных к значимым объектам КИИ, до вступления в силу ФЗ-187 от 26.07.2017.

Взаимодействие с ГОССОПКА (НКЦКИ) организуется в соответствии с вышеприведенными приказами ФСБ России, при этом необходимо учитывать, что информация передается обо всех инцидентах, происшедших на всех объектах КИИ, не только значимых.

Для обеспечения безопасности значимых объектов КИИ, являющихся информационными системами персональных данных, учитываются Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119 (Собрание законодательства Российской Федерации, 2012, N 45, ст. 6257).

Для обеспечения безопасности значимых объектов, являющихся государственными информационными системами, учитываются Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. №17.

ПРИЛОЖЕНИЕ 2

ПЕРЕЧЕНЬ ИСТОЧНИКОВ ИНФОРМАЦИИ.

1. Доктрина энергетической безопасности Российской Федерации, утверждена Указом Президента РФ от 13.05.2019 г. №216

2. Киберопасность как одна из стратегических угроз энергетической безопасности России. Массель Л.В., Воропай Н.И., Сендеров С.М., Массель А.Г. // Вопросы кибербезопасности. № 4(17) - 2016. стр. 2 – 9.

3. ГОСТ ISO/IEC 27032:2012 “Information technology — Security techniques — Guidelines for cybersecurity”, ГОСТ Р 56205-2014 “Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы”.

4. https://www.rosbalt.ru/world/2020/01/16/1822985.html?utm_source=yxnews&utm_medium=desktop&utm_referrer=https%3A%2F%2Fyandex.ru%2Fnews.

5. https://cnews.ru/news/top/2019-04-05_rossiya_provalilas_v_globalnom_rejtinge_kiberbezopasnosti.

6. Об участии Министерства энергетики РФ в конференциях по вопросам кибербезопасности промышленных объектов (https://minenergo.gov.ru/node/15857).

7. Правовое регулирование информационной безопасности в Российской Федерации. Мысев А.Э., Морозов Н.В. // Отечественная юриспруденция, 2019, стр. 51-55.

8. PROTECTION OF ‘CRITICAL INFRASTRUCTURE’ AND THE ROLE OF INVESTMENT POLICIES RELATING TO NATIONAL SECURITY. May 2008 http://www.oecd.org/daf/inv/investment-policy/40700392.pdf

9. Forging a Common Understanding. Shared Narrative, March 2014. https://www.dhs.gov/sites/default/files/publications/critical-five-shared-narrative-critical-infrastructure-2014-508.pdf

10. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.0. February 12, 2014 https://iapp.org/media/pdf/resource_center/NIST_Framework.pdf?fbclid=IwAR3oCmRXBYJFZzXTbPmHAWSIUuPTMnkUmt3d2Hi4Kdde4SejImul86mRhAs

11. CII-Act-508 https://www.dhs.gov/sites/default/files/publications/CII-Act-508.pdf

12. Methodologies for the identification of Critical Information Infrastructure assets and services. Guidelines for charting electronic data communication networks. December 2014 https://www.enisa.europa.eu/publications/methodologies-for-the-identification-of-ciis

13. ENISA issues methodologies for the identification of Critical Information Infrastructure (CII) services in communication networks. Published on February 23, 2015 https://www.enisa.europa.eu/news/enisa-news/how-critical-is-a-critical-information-infrastructure

14. Critical Information Infrastructures Protection approaches in EU. July 2015. https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproachesNCSS.pdf

EnergyNet

ЦЕНТР КОМПЕТЕНЦИЙ «КИБЕРБЕЗОПАСНОСТЬ»

ОБЪЕДИНЯЕМ КОМПЕТЕНЦИИ И ФОРМИРУЕМ СИСТЕМНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

Российское Энергетическое Агентство · НЕФТИ и ГАЗА · iGrids · Системный оператор Единой энергетической системы · kaspersky · ANGARA technologies group · СИСТЕМА · INFOWATCH · Ростелеком Солар